

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: M. NISHIOKA, et al

Serial No.: 10/046,224

Filing Date: January 16, 2002

or: PUBLIC-KEY CRYPTOGRAPHIC SCHEMES SECURE AGAINST AN
ADAPTIVE CHOSEN CIPHERTEXT ATTACK IN THE STANDARD
MODEL

Examiner: Not assigned

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §1.97 & 1.98

Assistant Commissioner
for Patents
Washington, D.C. 20231

February 26, 2002

Sir:

In the matter of the above-identified application, applicants are submitting herewith copies of the documents listed in the attached form equivalent to Form PTO-1449 for the Examiner's consideration.

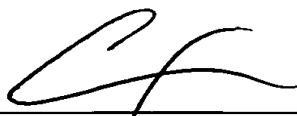
This information disclosure statement is being submitted within three months of the filing date.

Each of the documents listed on the attached form equivalent to Form PTO-1449 is in the English language.

It is respectfully requested that this information disclosure statement be considered by the Examiner.

Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to the deposit account of Antonelli, Terry, Stout & Kraus Deposit Account No. 01-2135 (500.41092X00) please credit any excess fees to such deposit account.

Respectfully submitted,



Carl I. Brundage
Registration No. 29,621
ANTONELLI, TERRY, STOUT & KRAUS, LLP

CIB/jdc
(703) 312-6600

FORM PTO-1449 U.S. Department of Commerce
(Rev. 4/92) Patent and Trademark Office

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use several sheets if necessary)

ATTY. DOCKET NO.

500.41092X00

SERIAL NO.

10/046,224

APPLICANT

M. NISHIOKA, et al

FILING DATE

January 16, 2002

GROUP

Not assigned

U.S. PATENT DOCUMENTS

DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT
					YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

V.S. Miller, "Use of Elliptic Curves in Cryptography", Proc. Of Crypto' 85, LNCS218, Springer-Verlag, pp. 417-426 (1985).
S. Goldwasser et al "Probabilistic Encryption, JCSS, 28, 2, pp. 270-299 (1984).
M. Blum et al, "An Efficient Probabilistic Public-Key Encryption Scheme which hides all partial Information", Proc. Of Crypto '84, LNCS196, Springer-Verlag, pp. 289-299 (1985).

EXAMINER

DATE CONSIDERED

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449 U.S. Department of Commerce
(Rev. 4/92) Patent and Trademark Office

ATTY. DOCKET NO.

SERIAL NO.

500.41092X00

10/046,224

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use several sheets if necessary)

APPLICANT

M. NISHIOKA, et al

FILING DATE

January 16, 2002

GROUP

Not assigned

U.S. PATENT DOCUMENTS

[illegible]

FOREIGN PATENT DOCUMENTS

[illegible]

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	S. Goldwasser et al, "Lecture Notes on Cryptography", http://www-cse.ucsd.edu/users/mihir/(1997) .
	T. Okamoto et al "A New Public-key Cryptosystem as Secure as Factoring, Proc. Of Eurocrypt '98, LNCS1403, Springer Veriag, pp. 308-318, (1998).
	M. Bellare et al, "Optimal Asymmetric Encryption How to Encrypt with RSA, Proc., of Eurocrypt '94, LNCS950, Springer Verlag, pp. 92-111 (1994).

EXAMINER

DATE CONSIDERED

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449 U.S. Department of Commerce
(Rev. 4/92) Patent and Trademark Office

ATTY. DOCKET NO.

SERIAL NO.

500.41092X00

10/046,224

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use several sheets if necessary)

APPLICANT

M. NISHIOKA, et al

FILING DATE

January 16, 2002

GROUP

Not assigned

FEB 26 2002

U.S. PATENT DOCUMENTS

EXAMINER	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT
					YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	R. Cramer et al "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack, Proc. Of Crypto '98, LNCS1462, Springer-Verlag, pp. 13-25, (1998).
	M. Bellare et al "Relations Among Notions of Security for Public-key Encryption Schemes, Proc. Of Crypto '98, LNCS1462, Springer Verlag, pp. 26-45 (1998).

EXAMINER

DATE CONSIDERED

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered.
Include copy of this form with next communication to applicant.